

Autorisation intelligente sur la plate-forme ASR9000

Contenu

[Introduction](#)

[Vue supérieure](#)

[Traditionnel contre des exécutions intelligentes d'autorisation](#)

[Vue opérationnelle](#)

[Interface web/portail](#)

[Configuration](#)

[Autorisation traditionnelle](#)

[Autorisation intelligente](#)

[L'anatomie et l'écoulement de l'application](#)

[Déploiement, configuration, et options](#)

[Configurez le proxy HTTP](#)

[Configurez la passerelle de transport](#)

[Configurez le VRF](#)

[Configurez le HTTP](#)

[Sortie détaillée de Fonction Call Home](#)

[Options de configuration Non-intelligentes d'autorisation de Fonction Call Home](#)

[Debug](#)

[Syslog](#)

[Processus de Fonction Call Home](#)

[Contrôle de Smartlic \(agent logiciel\)](#)

[Contrôle de processus de Licmgr](#)

[Suivis de personne à charge de plate-forme](#)

[Activez le debug](#)

[Chance et extrémités](#)

[Informations connexes](#)

Introduction

Ce document décrit la configuration du logiciel, l'exécution, et le dépannage intelligents d'autorisation sur la version 5.2.0 et ultérieures du Cisco IOS® XR. L'autorisation intelligente a été développée afin de s'adresser à la Gestion de conditions d'autorisation pour différentes caractéristiques et applications qui fonctionnent sur des Plateformes de Cisco et des systèmes d'exploitation (systèmes d'exploitation).

L'application d'autorisation intelligente fonctionne non seulement sur ASR9000 (ASR9K) pour le Cisco IOS XR, mais également sur les diverses Plateformes qui exécutent le Cisco IOS et les systèmes d'exploitation de Cisco IOS XE. Cette application simple réduit considérablement l'effort requis pour gérer les périphériques, les systèmes, et les Plateformes divers de Cisco et apporte la simplicité si nécessaire autoriser la Gestion, les autorisations, et les coûts d'exploitation.

La méthode utilisée par l'application d'autorisation intelligente est une méthode dynamique de « traction » ; le périphérique ASR9K initie l'appel et *tire les* informations des serveurs de backend de Cisco. Cisco centralisent des serveurs n'initiera pas n'importe quel appel ou connexion à n'importe quel périphérique, mais répond toujours quand les demandes de connexion proviennent les périphériques qui voudraient enregistrer et recevoir l'autorisation.

La première installation est sécurisée et facile avec l'intervention manuelle très petite de l'opérateur des dispositifs et peut être automatisée pour les environnements plus grands avec un d'ordres de gestion régulier d'outil (TCL) ou le python s'attendent au script. Les structures de compte-rendu fournies par des serveurs de backend de Cisco, accessibles par l'intermédiaire d'un navigateur régulier, aideront les clients avec la comptabilité de leur inventaire des périphériques, les caractéristiques se sont déployées autorisé et hors de la conformité (OOC) et déplacent dynamiquement leurs ressources autour sans reprovision du besoin ou nécessitent le support.

Vue supérieure

HTTP standard d'utilisations intelligentes d'autorisation/HTTP sécurisé (HTTPS) comme mécanisme de transport afin d'atteindre les serveurs de backend de Cisco. Techniquement parlant, il y a seulement une ligne de configuration qui est nécessaire afin d'activer la caractéristique intelligente d'autorisation sur le périphérique ASR9K :

```
RP/0/RSP0/CPU0:SAMDD(admin-config)#license smart enable
```

Les par défaut de périphérique à HTTPS transportent et sur demande d'enregistrement réussie, questionne immédiatement les serveurs principaux pour l'autorisation. Il renvoie l'un ou l'autre autorisé, qui signifie le périphérique a le permis pour la caractéristique, ou OOC, qui signifie que l'autorisation n'est pas présente, des disparus, ou expiré.

Note: L'état de conformité aux licences n'affectera pas la fonctionnalité du périphérique de quelque façon. L'application d'autorisation intelligente en cours est basée sur un tableau d'honneur et informe l'administrateur par l'intermédiaire du Syslog ou la console se connecte quant à la conformité ou à l'état OOC. Il n'y a aucune entrave de fonctionnalité de quelque façon due à l'autorisation ou au manque s'y rapportant. Cependant, Cisco encourage la conformité qui donne beaucoup plus de visibilité aux clients quant à leur inventaire des périphériques, consommation de permis, des caractéristiques utilisées par périphérique et dans l'agrégat/grand total, et ainsi de suite.

L'autorisation intelligente peut coexister avec l'autorisation traditionnelle, mais seulement un d'entre eux peut être en activité à un moment donné. Vous pouvez commuter entre eux facilement avec l'ajout ou la suppression de la configuration de l'avion de gestion. Le système ASR9K n'exige d'aucune recharge ou reprise pour ce « commutateur » d'avoir lieu. L'autorisation traditionnelle sera remplacée complètement avec l'autorisation intelligente dans des versions futures.

Si un périphérique ASR9K n'utilise pas une caractéristique qui exige l'autorisation, alors automatiquement le système est dans l'état autorisé et aucune autre mesure ne doit être prise. Seulement sur la « configuration » d'une caractéristique qui exige un permis l'essai de système saisira le permis dynamiquement des serveurs de backend de Cisco.

Traditionnel contre des exécutions intelligentes d'autorisation

Voici quelques différences entre les modèles d'autorisation. Notez que seulement un d'entre eux est en activité à un moment donné.

(Noeud verrouillé) autorisation traditionnelle

Vous devez obtenir le permis et manuellement l'installer sur chaque périphérique par l'intermédiaire du fichier PAK.

Les permis attachés au châssis, se déplaçant, ou reprovisioning exigent la sauvegarde ou la réinstallation. Toutes sont des exécutions manuelles qui consomment le temps.

permis Noeud-verrouillé - le permis est associé avec un appareil spécifique/emplacement.

Pas commun installez

l'emplacement de base afin de visualiser des permis achetés ou des tendances d'utilisation de logiciel.

La comptabilité de permis doit être mise à jour pour le différents châssis/systèmes manuellement.

Le permis supplémentaire exige un nouveau fichier et l'intervention manuelle/interaction PAK avec le périphérique.

Aucun moyens faciles de transférer des permis d'un périphérique à l'autre.

Autorisation (dynamique) intelligente

Aucune installation de logiciel n'est nécessaire/nécessaire. Le périphérique initie une session de Fonction Call Home HTTP/HTTPS demande les permis qu'elle l'utilise et est configuré pour.

Permis attachés à votre compte. Unconfigure la caractéristique qui est utilisée dans le châssis en cours et modifient la caractéristique sur un nouveau châssis qui doit utiliser le même permis. Un reprovision se produit dynamiquement quand le nouveau périphérique initie une demande HTTP/HTTPS par l'intermédiaire du processus de Fonction Home.

Autorisez les groupes créés déjà dans le compte client, qui sont com particularité de société et peuvent être utilisés avec n'importe quel périphérique ASR9K à votre société.

Des permis sont enregistrés sécurisé sur des serveurs de backend de Cisco, 24x7x365 accessible. Le compte de permis est par compte client/groupe et beaucoup de périphériques peuvent faire partie du même groupe.

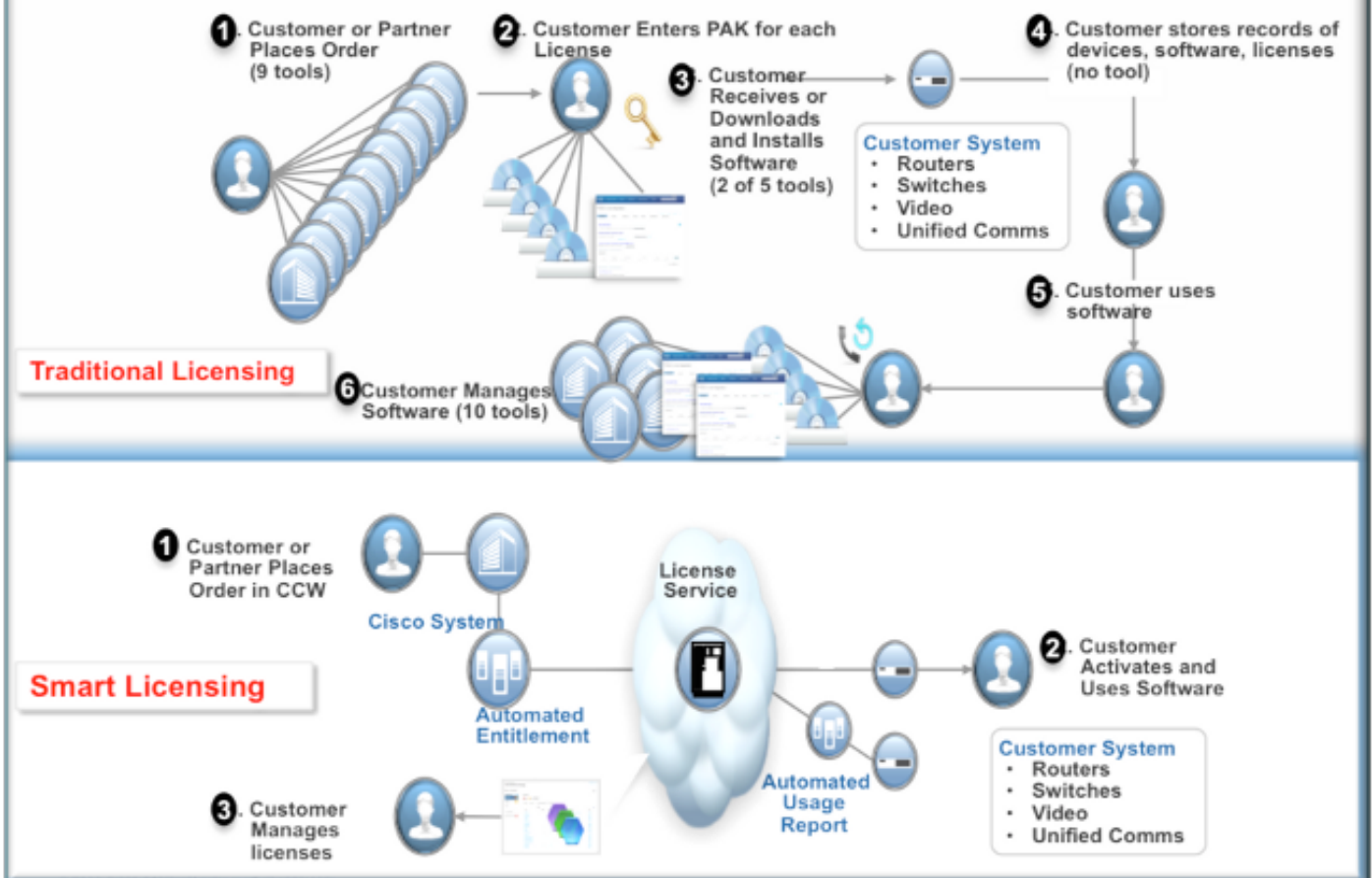
Le permis supplémentaire peut être transféré par l'intermédiaire d'un navigateur Web que les points à l'URL de Cisco et au compte ont créé dans des serveurs principaux. Exécutions fondamentalement de point de clic.

Des permis peuvent être déplacés entre les exemples de produit sans N'IMPORTE QUELLE installation de logiciel. Vous pouvez également des permis d'un groupe sur l'autre facilement avec une interface web

Vue opérationnelle

Ce diagramme affiche la comparaison entre les deux systèmes de licence.

Systems View; Traditional V.S. Smart Licensing



Les étapes intelligentes d'autorisation sont très faciles et intuitives. Quand vous achetez l'équipement/périphérique, vous pouvez commander les permis que vous avez besoin en même temps ou les commandez plus tard. Lors de l'exécution de l'achat et du ravitaillement des permis par Cisco :

- Cisco te fournit un nom d'utilisateur, un mot de passe, et un uniform resource locator (URL) pour accéder à des données de licence par l'intermédiaire d'un navigateur Web 24x7.
- Ce compte gère des permis, génère des états, des périphériques de groupes, fait des groupes des permis et de n'importe quel autre besoin organisationnel qui facilite les besoins opérationnels du client/d'organisation.
- Le compte permet au client pour générer un *idtoken*, qui identifie seulement le périphérique de client et l'autorisation d'autorisation achetés. Le jeton peut être valide d'un jour à un an. L'*idtoken* peut être retiré, supprimé, et recréé par le client à tout moment. C'est un modèle d'aide.
- Le client utilise l'*idtoken* généré dans le compte fourni par Cisco afin d'enregistrer un périphérique ou mille périphériques, car il n'y a aucune limite sur combien de périphériques peuvent utiliser le même jeton. Plus de conseils sur l'utilisation efficace de cette caractéristique sont fournis dans ce document.
- L'enregistrement de périphérique est persistant et survit à travers des recharges et des mises à jour du système. Le périphérique ASR9K peut être forcé pour reregister avec le vieux

idtoken ou plus nouvel si on souhaite, en cas de n'importe quelle perte.

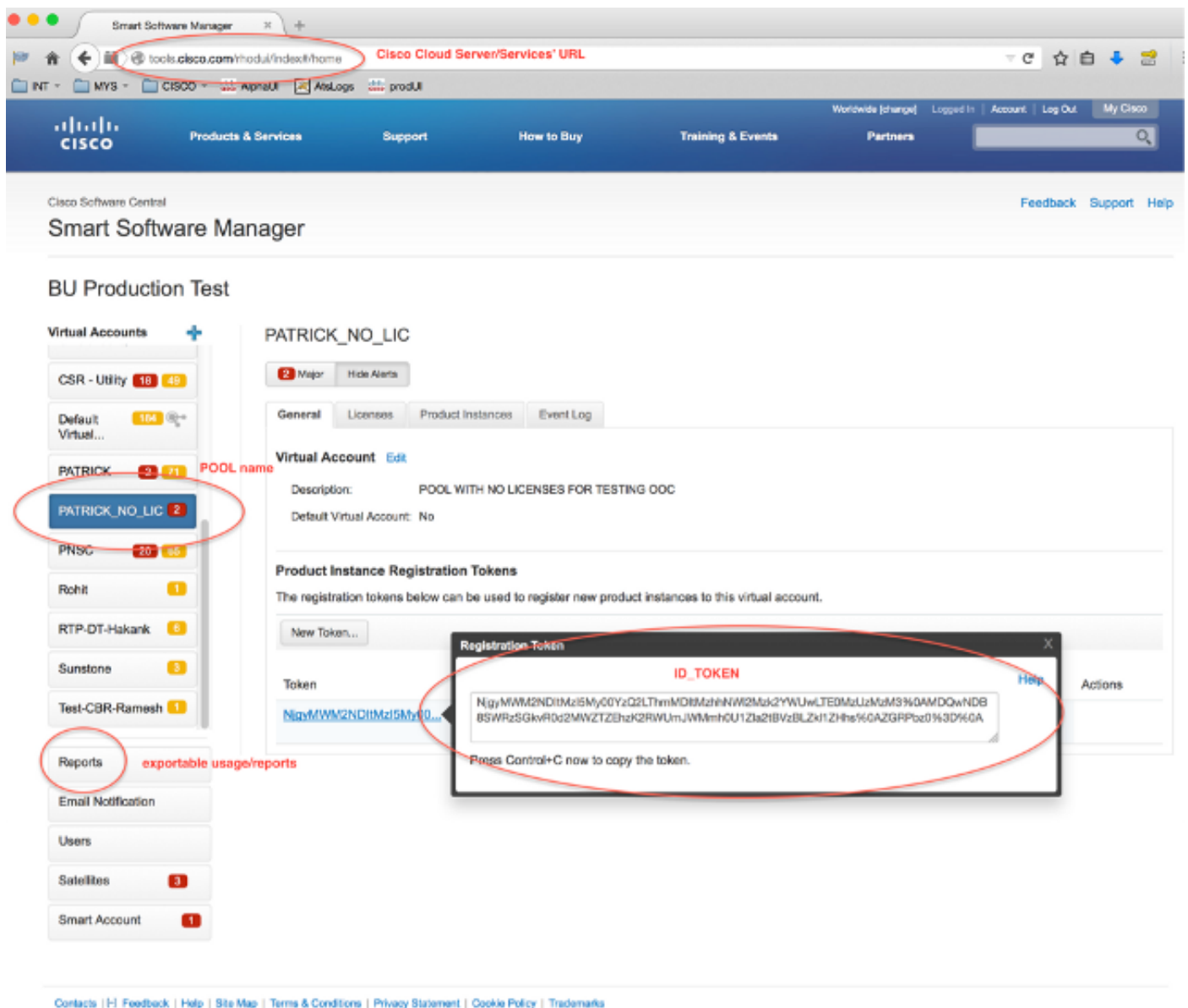
- Aucune intervention n'est nécessaire après enregistrement, le système ASR9K vote périodiquement le compte qu'il s'est inscrit avec à la conformité. Si le système est OOC un Syslog est généré pour avertir l'utilisateur.

Interface web/portail

Voici une visite rapide de l'interface web où la procédure d'enregistrement commence :

Le groupe virtuel de permis de compte aka est utilisé logiquement pour loger et organiser des permis par besoin d'une organisation. C'est un conteneur de permis, les périphériques enregistrés pour les caractéristiques qui exigent un permis. Vous pouvez créer un groupe par site, par service, et ainsi de suite.

Des permis peuvent être facilement transférés d'un groupe à l'autre.



Idtoken est une *clé* générée par *ce* compte, qui est utilisé pour enregistrer les périphériques ASR9K. Il peut être valide d'un jour à un an. La seule utilisation pour le jeton est d'enregistrer le

périphérique et ensuite cela elle n'est pas nécessaire. Le jeton est un flot de texte qui peut être copié dans un script TCL ou de python afin d'automatiser l'enregistrement de périphérique distant.

Par exemple, vous pouvez créer un jeton pour un jour et l'envoyer à un site distant à utiliser par les mains distantes pour l'enregistrement de périphérique. Il expire dans un jour et les mains de distant ne peuvent pas l'employer afin de n'enregistrer aucun autre périphérique. Même si il est utilisé pour enregistrer les périphériques qui n'appartiennent pas à votre société, vous verrez facilement le périphérique dans le **produit citer l'onglet** et pouvez agir afin de retirer le permis.

L'état génère dynamiquement de diverses formes d'inventaire et peut être exporté dans un format d'Exceler à l'utilisation, à la comptabilité, ou à l'analyse hors ligne.

L'onglet de permis affiche les permis demandés par de divers périphériques ASR9K, qui affiche le *compte* et l'état de chaque permis. L'élément de lien de *transfert* peut être utilisé quand vous le cliquez sur en fonction directement et transférez facilement des permis à et de n'importe quel groupe dans le compte.

The screenshot shows the Cisco Smart Software Manager interface. On the left, there is a sidebar with 'Virtual Accounts' including 'PATRICK_NO_LIC' which is selected. The main content area displays the 'Licenses' tab for 'PATRICK_NO_LIC'. A table lists licenses with columns for License, Quantity, In Use, Surplus (+)/ Shortage (-), Alerts, and Actions. Two rows are visible, both showing a shortage of 1 unit. A red star highlights the 'Event Log' tab, and a red circle highlights the 'Transfer...' link in the Actions column. A red box highlights the first row of the table.

License	Quantity	In Use	Surplus (+)/ Shortage (-)	Alerts	Actions
ASR 9000 24X10G LC Advanced Optics License	0	1	-1	Insufficient Licenses Xfer license from another pool	Transfer...
ASR 9000 36X10G LC Advanced Optics License	0	1	-1	Insufficient Licenses	Transfer...

Les activités d'enregistrements d'onglet de journal d'événements des périphériques contre le groupe avec un Syslog tapent le format et se connectent des actions chaque périphérique ou l'utilisateur du compte prend, comme l'enregistrement, la radiation, et ainsi de suite. L'interface est facile et intuitive pour la navigation ou l'élimination des imperfections.

Configuration

Cet exemple jette un regard comment améliorer de l'autorisation traditionnelle à l'autorisation intelligente. Notez que l'autorisation dans certains cas intelligente pourrait être le par défaut.

Autorisation traditionnelle

Afin de vérifier l'autorisation traditionnelle, quelques commandes peuvent être exécutées de l'*avion d'admin*. Voici quelques uns qui ont différentes sorties une fois comparés à l'autorisation intelligente.

Note: L'autorisation traditionnelle est le mode par défaut d'autorisation dans des versions 5.3.0 de Cisco IOS XR et plus tôt.

```
RP/0/RSP1/CPU0:ROA(admin)#show license pools
```

```
Pool: Owner
Feature: A9K-24X10-OPT-LIC A9K-24X10-VID-LIC A9K-24X10G-AIP-SE A9K-24X10G-AIP-TR
A9K-2X100-OPT-LIC A9K-2X100-VID-LIC A9K-2X100G-AIP-SE A9K-2X100G-AIP-TR
A9K-36X10-OPT-LIC A9K-36X10-VID-LIC A9K-36X10G-AIP-SE A9K-36X10G-AIP-TR
A9K-400G-AIP-SE A9K-400G-AIP-TR A9K-400G-OPT-LIC A9K-400G-VID-LIC
A9K-800G-AIP-SE A9K-800G-AIP-TR A9K-800G-OPT-LIC A9K-800G-VID-LIC
A9K-ADV-OPTIC-LIC A9K-ADV-VIDEO-LIC A9K-AIP-LIC-B A9K-AIP-LIC-E
```

```
RP/0/RSP1/CPU0:ROA(admin)#show license allocated
```

```
FeatureID: A9K-800G-AIP-SE (Slot based, Permanent)
Total licenses 1
Status: Allocated 1
Pool: Owner
Total licenses in pool: 1
Status: Operational: 1
Locations with licenses: (Active/Allocated) [SDR]
0/0/CPU0 (0/1) [Owner]
```

Un sous-ensemble de commandes traditionnelles d'autorisation peut également être exécuté de l'*avion d'exécutif*, mais c'est une bonne idée de les exécuter de l'*avion d'admin*, qui a la liste complète.

```
RP/0/RSP1/CPU0:ROA#show license ?
```

```
WORD      Feature ID
active     Currently checked-out/being used by applications.
allocated  Allocated to a slot but not used.
available  Not currently active.
evaluation Display the evaluation licenses.
expired    Display evaluation licenses already expired.
location   Show information for a specific location
log        The operational or administrative logs.
|         Output Modifiers
<cr>
```

Autorisation intelligente

L'autorisation intelligente n'a pas été activée encore, mais est ce ce que le système affiche.

Quoiqu'aucune configuration ne soit appliquée, le profil intégré par défaut du *call_home* utilise HTTPS, que les points aux serveurs de backend de Cisco par l'intermédiaire de la gestion des systèmes met en communication. Voyez plus sur le *call_home* plus tard dans ce document.

```
RP/0/RSP1/CPU0:ROA#show run call-home
% No such configuration item(s)
```

```
RP/0/RSP1/CPU0:ROA#show call-home detail | i https
http proxy: Not yet set up
HTTP address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Pour un strict minimum de configuration, vous avez besoin seulement d'étapes 1 et 4. Le reste des étapes sont pour information, la vérification, et l'enregistrement.

1. En *mode d'admin*, sélectionnez ces commandes :

```
RP/0/RSP1/CPU0:ROA(admin-config)#license smart enable
RP/0/RSP1/CPU0:ROA(admin-config)#commit
```

2. Dans le *mode d'exécution* configurez plus de molettes, telles que l'adresse e-mail, ou utilisez ce profil par défaut qui est généré automatiquement quand la configuration d'admin est commise.

```
RP/0/RSP1/CPU0:ROA#show run call-home
call-home
service active
contact-email-addr sch-smart-licensing@cisco.com
profile CiscoTAC-1
active
destination transport-method http
```

3. En *mode d'admin*, vérifiez la version intelligente d'autorisation :

```
RP/0/RSP1/CPU0:ROA(admin)#show license version
Cisco Smart Licensing Agent, Version 1.1.4_throttle/16
```

4. En *mode d'admin*, sélectionnez cette commande :

```
RP/0/RSP1/CPU0:ROA(admin)#license smart register idtoken
NjgyMWM2NDItMzI5My00YzQ2LTNmMDItMzhhNWl2Mzk2YWUwLTE0MzUzMzM3%
0aMDQwNDB8SWRzSGkvR0d2MWZTZEhzK2RWUmJWMMh0U1ZlIa2tBVzBLZk1lZHhs%0AZGRPbz0%3D%0A ?
force Force Registration
<cr>
```

```
license smart register: Registration process is in progress. Please check
the syslog for the registration status and result
```

La force de mot clé remplace et élimine l'intégralité d'informations en vue de le périphérique qui a été enregistré précédemment. La force de mot clé devrait être utilisée économiquement et dans des cas particuliers. Alternativement, l'interface utilisateur d'utilisateur web peut être utilisée afin de retirer le périphérique du compte.

5. Requête pour le statut de l'exécution :

```
RP/0/RSP1/CPU0:ROA(admin)#show license register-status
Registration Status: Completed
Registration Start Time: Wed Dec 17 2014 13:07:23 PST
Next ID Cert Renew Time: Mon Jun 15 2015 14:07:45 PST
Next ID Cert Expiration Time: Thu Dec 17 2015 13:01:41 PST
Last Response Time: Wed Dec 17 2014 13:07:45 PST
Last Response Message: OK: OK
```

Si l'état « n'est pas terminé », vous verrez des messages sur la console ou le Syslog. Voici le message réussi de Syslog :

```
RP/0/RSP1/CPU0:ROA(admin)#show license register-status
Registration Status: Completed
Registration Start Time: Wed Dec 17 2014 13:07:23 PST
Next ID Cert Renew Time: Mon Jun 15 2015 14:07:45 PST
Next ID Cert Expiration Time: Thu Dec 17 2015 13:01:41 PST
Last Response Time: Wed Dec 17 2014 13:07:45 PST
Last Response Message: OK: OK
```

6. Sur ce système il y a peu de caractéristiques configurées qui exigent des permis et cette sortie indique l'état de « hors de la conformité » :


```
RP/0/RSP1/CPU0:ROA(admin)#show license entitlement | i Tag | e Not | u sort
```

```
Tag: regid.2014-04.com.cisco.A9K-24X10-OPT-LIC,  
1.0_66d3ccf7-a374-4409-a3f9-6bc56d645f1c, Version: 1.0, Enforce Mode:  
Out of compliance
```

```
Tag: regid.2014-04.com.cisco.A9K-24X10-VID-LIC,1.0_9f03b94f-3c76-4a39-82f2  
-1b53cdf5cb15, Version: 1.0, Enforce Mode: Out of compliance
```

```
Tag: regid.2014-04.com.cisco.A9K-24X10G-AIP-TR,1.0_e5d7cec3-e8e3-43c6-88c9  
-a113b76679f8, Version: 1.0, Enforce Mode: Out of compliance
```

```
Tag: regid.2014-06.com.cisco.A9K-2X100-OPT-LIC,1.0_0f74bb00-42af-4c4d-b162  
-bcb346c7510a, Version: 1.0, Enforce Mode: Out of compliance
```

```
Tag: regid.2014-06.com.cisco.A9K-2X100-VID-LIC,1.0_a482b964-6371-4aad-8e82  
-2083c5749205, Version: 1.0, Enforce Mode: Out of compliance
```

```
Tag: regid.2014-06.com.cisco.A9K-2X100G-AIP-SE,1.0_ce447831-e4af-4def-a98b  
-3297fab65561, Version: 1.0, Enforce Mode: Out of compliance
```

```
Tag: regid.2014-06.com.cisco.A9K-36X10-OPT-LIC,1.0_92a8597a-f591-4afc-adeb  
-9b212cee11be, Version: 1.0, Enforce Mode: Out of compliance
```

7. Regardez les commandes que vous avez utilisées dans l'autorisation traditionnelle, qui ont la sortie différente. L'autorisation intelligente OU l'autorisation traditionnelle CLI est disponible à un moment donné, pas chacun des deux. **Le nom du pool** est utilisé pour organiser/classe des périphériques par catégorie. Vous pouvez utiliser un groupe par région/zone géographique, ou service ou domaine fonctionnel, ou groupements financiers, et ainsi de suite. Chaque société peut décider comment elles voudraient classer des permis. Notez également qu'il est très facile à utiliser votre navigateur normal afin de visualiser, changer, ou déplacer des permis entre les groupes, ajouter ou changer les comptes de permis, et faire tellement facilement sans n'importe quelle aide de Cisco, indépendamment, vingt-quatre heures sur vingt-quatre.

```
RP/0/RSP1/CPU0:ROA(admin)#show license pool
```

```
Assigned Pool Info: PATRICK_NO_LIC
```

8. D'ici en fonction, les contrôles du système chaque jour pour la conformité automatiquement. S'il y a une panne, le système essaye toutes les 20 minutes pendant quatre heures et ensuite cela une fois par jour pendant 30 jours. Des messages de Syslog sont imprimés, qui indiquent la Connectivité, accessibilité, transmission, raisonne et ainsi de suite pour des pannes. L'élimination des imperfections est discutée plus tard dans ce document.
9. Afin de radier de l'immatriculation le périphérique, sélectionnez ces commandes :

```
RP/0/RSP1/CPU0:ROA(admin)#license smart deregister
```

```
license smart deregister: Success
```

```
License command "license smart deregister " completed successfully.
```

```
RP/0/RSP1/CPU0:ROA(admin)#show license register-status
```

```
Registration Status: Not Registered
```

10. Afin de découvrir quels permis sont disponibles sur un châssis donné, sélectionnez cette commande :

```
RP/0/RSP1/CPU0:ROA(admin)#show license features
```

```
Platform Feature ID:
```

```
A9K-ADV-OPTIC-LIC
```

```
A9K-ADV-VIDEO-LIC
```

```
A9K-iVRF-LIC
```

```
A9K-AIP-LIC-B
```

```
A9K-AIP-LIC-E
```

```
A9K-MOD80-AIP-TR
```

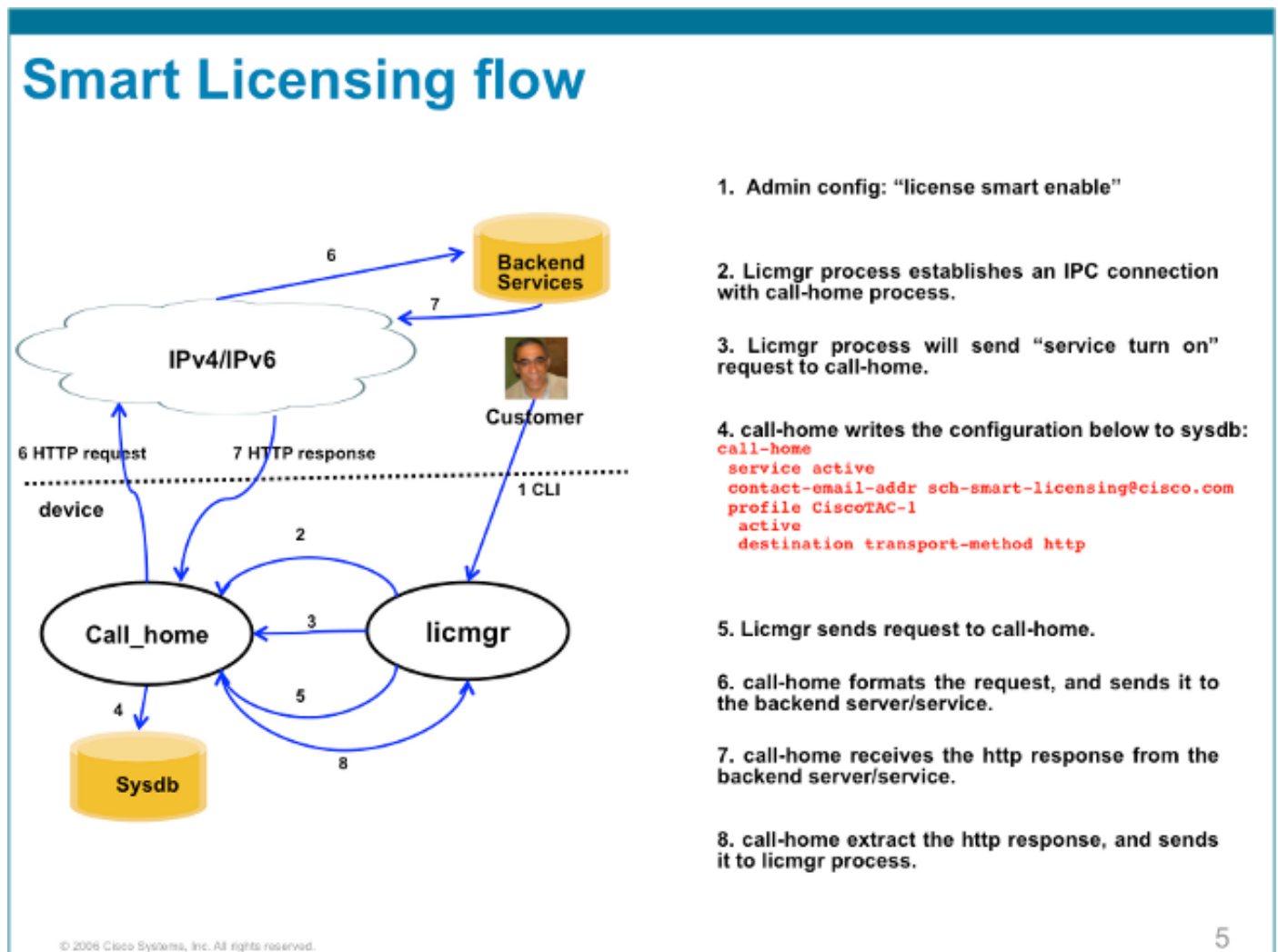
```
A9K-MOD80-AIP-SE
```

```
A9K-MOD160-AIP-TR
```

```
A9K-MOD160-AIP-SE
```

L'anatomie et l'écoulement de l'application

Afin de comprendre les mécanismes de l'application, vous devez avoir une compréhension de base de ses composants. Pour l'exécution ou le déploiement du logiciel, cependant, aucune connaissance préalable n'est nécessaire autre que pour suivre les instructions éditées. Cette section est destinée davantage pour l'équipe technique et les ingénieurs qui voudraient connaître les détails.



Déploiement, configuration, et options

L'autorisation intelligente peut être déployée dans plusieurs scénarios dépendants sur les conditions requises en ce qui concerne la Sécurité, la gestionnabilité, et le mode opérationnel du client.

Exemple :

- Vous pourriez choisir de ne pas permettre à l'ASR9K pour se connecter « directement » aux serveurs de nuage/backend de Cisco. Dans ce cas vous pouvez utiliser un serveur de « proxy » sur vos sites et gérer le Pare-feu, la circulation, et comment les adaptations intelligentes d'application d'autorisation dans la Sécurité de l'organisation a besoin. Ceci peut

être facilement installé par l'intermédiaire du logiciel d'Open Source Apache qui fonctionne sur des systèmes d'exploitation de Windows ou Linux.

- Ou vous pourriez vouloir avoir tous vos périphériques ASR9K connectés à un hôte d'agrégateur qui peut recevoir toutes les demandes locales de tous les périphériques ASR9K avant que vous leur fassiez suivre des serveurs de backend de Cisco. C'est un travail pour le logiciel de passerelle de transport qui les passages sur le Linux et Windows et est disponible pour le téléchargement au [téléchargement de Passerelles de transport Cisco](#).
- Ou vous pourriez vouloir opérer totalement off-line avec sur-Prem le logiciel que les passages sur le Linux et Windows et te permet pour avoir seulement « ceci sur-Prem l'hôte » pour faire parler pour l'échange d'informations d'autorisation avec le nuage de Cisco et consécutivement pour fournir des informations aux périphériques d'extrémité quant à leur état de conformité. Ce logiciel sera disponible dans la version 5.3.1 ou plus tard.

En plus du soutien de HTTPS, le logiciel peut également être configuré pour s'exécuter dans une configuration virtuelle d'expédition de routage (VRF) qui permet un plus grand niveau de contrôle au-dessus de la façon dont les informations d'autorisation sont transportées.

En outre, l'IPv6 est pris en charge à la façon des indigènes et exige seulement une adresse IP6 valide sur le communciate de système avec des serveurs de backend de Cisco au-dessus de l'Internet.

Ces configurations supposent que l'ASR9K est configuré avec le Système de noms de domaine (DNS) ou l'hôte du domaine IPv4/IPv6 de sorte qu'il puisse résoudre des noms d'hôte afin d'atteindre le réseau extérieur.

La configuration du Protocole NTP (Network Time Protocol) est nécessaire afin de garder le système en phase avec les serveurs principaux de certificat.

```
RP/0/RSP0/CPU0:ROA#show run domain
domain name cisco.com
domain list cisco.com
domain name-server 171.70.168.183
domain name-server 2001:420:68d:4001::a
```

```
RP/0/RSP0/CPU0:ROA#show run | i ipv6 host
Building configuration...
domain ipv6 host tools.cisco.com 2001:420:1101:5::a
```

Configurez le proxy HTTP

La configuration d'Apache est hors de portée de ce document, mais il y a beaucoup de bons documents sur l'Internet qui peut marcher vous par les étapes. Afin d'expliquer la fonctionnalité, Apache est configuré pour un proxy simple sur le port 80. Voyez la sortie de débogage du mod_proxy d'Apache affiché ici.

Pour intelligent l'autorisation, cependant, de la configuration est très simple, mentionne juste le nom et le port du serveur proxy. La configuration fera suivre simplement à la demande le serveur proxy au lieu de contacter les serveurs de backend de Cisco directement. Le serveur proxy contactera les serveurs au-dessus de Qu'est ce que transport est configuré pour expédier les demandes ; HTTPS est recommandé. Indépendamment du **port 80 de mybastion.cisco.com de proxy HTTP**, pas n'importe quelle autre configuration est exigée.

```
RP/0/RSP0/CPU0:ROA#show run call-home
call-home
service active
http-proxy mybastion.cisco.com port 80
contact-email-addr sch-smart-licensing@cisco.com
profile CiscoTAC-1
active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http
```

Entrez dans le **permis d'admin de** commande d'enregistrement le **registre qu'intelligent idtoken le <idtoken>** et observez que la sortie affiche la demande/réponse faite par l'ASR9K. Notez les compteurs d'horodateurs et de colonne de succès.

```
RP/0/RSP0/CPU0:ROA#show call-home smart-licensing statistics
Success: Successfully sent and response received.
Failed : Failed to send or response indicated error occurred.
Inqueue: In queue waiting to be sent.
Dropped: Dropped due to incorrect call-home configuration.
```

Msg Subtype	Success	Failed	Inqueue	Dropped	Last-sent (GMT-08:00)
ENTITLEMENT	1	0	0	0	2015-01-12 21:06:56
DEREGISTRATION	0	0	0	0	n/a
REGISTRATION	1	0	0	0	2015-01-12 21:06:21
ACKNOWLEDGEMENT	1	0	0	0	2015-01-12 21:06:38

Voici un extrait des logs d'accès d'Apache qui affiche que la demande sort sur le port 443, protocole HTTPS.

```
RP/0/RSP0/CPU0:ROA#show call-home smart-licensing statistics
Success: Successfully sent and response received.
Failed : Failed to send or response indicated error occurred.
Inqueue: In queue waiting to be sent.
Dropped: Dropped due to incorrect call-home configuration.
```

Msg Subtype	Success	Failed	Inqueue	Dropped	Last-sent (GMT-08:00)
ENTITLEMENT	1	0	0	0	2015-01-12 21:06:56
DEREGISTRATION	0	0	0	0	n/a
REGISTRATION	1	0	0	0	2015-01-12 21:06:21
ACKNOWLEDGEMENT	1	0	0	0	2015-01-12 21:06:38

Configurez la passerelle de transport

Dans ce scénario l'application de passerelle de transport est installée sur un hôte de Windows ou Linux et configurée pour recevoir les demandes d'autorisation des périphériques ASR9K sur les sites du client et pour les transmettre par relais aux serveurs de backend de Cisco. Voir le pour en savoir plus du [déploiement et de guide utilisateur de passerelle de transport](#).

La configuration sur l'ASR9K est juste une ligne. Voici un échantillon ; consultez la documentation pour les configurations exactes requises pour votre environnement.

```
RP/0/RSP0/CPU0:ROA#show call-home smart-licensing statistics
Success: Successfully sent and response received.
Failed : Failed to send or response indicated error occurred.
Inqueue: In queue waiting to be sent.
Dropped: Dropped due to incorrect call-home configuration.
```

Msg Subtype	Success	Failed	Inqueue	Dropped	Last-sent (GMT-08:00)
ENTITLEMENT	1	0	0	0	2015-01-12 21:06:56
DEREGISTRATION	0	0	0	0	n/a
REGISTRATION	1	0	0	0	2015-01-12 21:06:21
ACKNOWLEDGEMENT	1	0	0	0	2015-01-12 21:06:38

Configurez le VRF

Les vrf laisse plus de contrôle du trafic d'administration et est presque transparent à l'autorisation intelligente. Cependant, une ligne configuration est nécessaire afin de faire le logiciel sous-jacent consulter la table de VRF plutôt que la table globale quand des essais intelligents de logiciel d'autorisation pour atteindre les serveurs de backend de Cisco.

La chaîne affichée ici est le nom de VRF configuré dans le système.

```
RP/0/RSP0/CPU0:ROA(config)#http client vrf MGMT
```

Configurez le HTTP

Le système fournit également le transport standard de HTTP aussi bien. La configuration est aussi simple que retirant le « s » du HTTPS avec la syntaxe identique.

```
RP/0/RSP0/CPU0:ROA#show run call-home
call-home
service active
profile CiscoTAC-1
active
destination address http http://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http
```

Sortie détaillée de Fonction Call Home

Un résultat témoin à vérifier si des travaux de Fonction Call Home correctement est affichés ici.

```
RP/0/RSP0/CPU0:ROA#show call-home detail
```

```
Current call home settings:
  call home feature : enable
  call home message's from address: mylab-roa@cisco.com ; optional, any address
  call home message's reply-to address: pasoltan@cisco.com ; optional,
recipient address

  vrf for call-home messages: Not yet set up ; Not supported natively yet

  contact person's email address: sch-smart-licensing@cisco.com ; default

  contact person's phone number: +1-408-526-8438 ; optional
  street address: 1550 Soltani Lane, Cisco System Drive, North Pole, NP 99709
  customer ID: Not yet set up
  contract ID: Not yet set up
  site ID: BUILDING20-125 ; optional

  source interface: Not yet set up ; can be configured to use a specific interface.
```

Mail-server[1]: Address: bastion.cisco.com Priority: 1 ; optional
Mail-server[2]: Address: 171.68.58.10 Priority: 10 ; optional
Mail-server[3]: Address: 173.37.183.72 Priority: 20 ; optional
http proxy: Not yet set up ; when configured will change.

Smart licensing messages: enabled

Profile: CiscoTAC-1 (status: ACTIVE) ; default profile supported.

Can not be renamed, deleted, but can be modified, activated, deactivated.

aaa-authorization: disable ; optional

aaa-authorization username: callhome (default) ; default

data-privacy: normal ; can be configured to use the hostname or not.

syslog throttling: enable

Rate-limit: 5 message(s) per minute

Snapshot command: Not yet set up

; Non-smart licensing configuration for alerts, data collection, defaults.

Available alert groups:

Keyword	State	Description
configuration	Enable	configuration info
environment	Enable	environmental info
inventory	Enable	inventory info
snapshot	Enable	snapshot info
syslog	Enable	syslog info

Profiles:

Profile Name: CiscoTAC-1

Profile status: ACTIVE

Profile mode: Full Reporting

Reporting Data: Smart Call Home, Smart Licensing

Preferred Message Format: xml

Message Size Limit: 3145728 Bytes

Transport Method: http

Email address(es): callhome@cisco.com

HTTP address(es): ; Only configuration needed if default is not desired.

<http://tools.cisco.com/its/service/oddce/services/DDCEService>

<https://tools.cisco.com/its/service/oddce/services/DDCEService>

Periodic inventory info message is scheduled every 23 day of the month at 11:2

Alert-group	Severity
environment	minor
inventory	normal

Syslog-Pattern	Severity
.*	critical

Options de configuration Non-intelligentes d'autorisation de Fonction Call Home

Vous pouvez configurer la Fonction Call Home pour faire la collecte des informations de Syslog et de diagnostic aussi bien que les vidages de mémoire, ou la faites envoyer des notifications électroniques pour des événements et ainsi de suite avec les les corvées intelligentes d'autorisation qu'elle se termine.

Vous pouvez visualiser votre information collectée de Fonction Call Home avec votre nom

d'utilisateur et mot de passe intelligent d'autorisation chez <https://tools.cisco.com/sch/reports/deviceReport.do>.

Voyez les documents joints dans la section « de l'information relative » pour plus d'informations sur la façon employer cette caractéristique afin de bénéficier votre environnement. Également un échantillon de notification électronique est dans la « chance et finit » la section.

Debug

Il n'y a des règles pas dures et rapides de mettre au point le logiciel intelligent d'autorisation dû à beaucoup de composants qui comportent le module. Cependant, quelques méthodes communes d'approche rétrécissent habituellement vers le bas les questions. Voici quelques suggestions.

Syslog

Regardez dans le Syslog d'abord. Vous obtiendrez quelques indices quant à quel composant devrait être vérifié d'abord. Dans ces messages vous voyez quelques questions de certificat et un manque d'envoyer des messages de HTTP de Fonction Call Home ; finalement la transmission est restaurée.

```
RP/0/RSP0/CPU0:ROA#sh log | i SMART
```

```
RP/0/RSP1/CPU0:Dec 17 20:01:28.522 : licmgr[308]: SMART_LIC-3-ID_CERT_RENEW_FAILED:  
ID certificate renewal failed: Response error: {"product_instance_identifieur":  
["ProductInstance '8baecfb5-2688-429b-8519-10a3f0dec6b5' is not valid"]}
```

```
RP/0/RSP1/CPU0:Dec 17 20:01:34.273 : licmgr[308]: SMART_LIC-3-AUTH_RENEW_FAILED:  
Authorization renewal with Cisco licensing cloud failed: Response error:  
LS_UNMATCH_SIGNED_DATA&colon; Signed data and certificate does not match
```

```
RP/0/RSP0/CPU0: Dec 17 18:26:24.009 : licmgr[314]: SMART_LIC-3-COMM_FAILED:  
Communications failure with Cisco licensing cloud: Fail to send out Call Home  
HTTP message
```

```
RP/0/RSP0/CPU0:Dec 17 18:28:03.057 : licmgr[314]: SMART_LIC-3-AGENT_REG_FAILED:  
Smart Agent for Licensing Registration with Cisco licensing cloud failed:  
Communication message send error
```

```
RP/0/RSP0/CPU0:Dec 17 18:30:09.247 : licmgr[314]: SMART_LIC-5-COMM_RESTORED:  
Communications with Cisco licensing cloud restored
```

```
RP/0/RSP0/CPU0:Dec 17 18:30:21.923 : licmgr[314]: SMART_LIC-6-AGENT_REG_SUCCESS:  
Smart Agent for Licensing Registration with Cisco licensing cloud successful
```

Cochez la **sortie de commande show** afin d'obtenir un traitement sur dans quel état la case/composant est. Voici que vous voyez la mobilité, l'IPSec (IPsec), et les permis Optiques.

```
RP/0/RSP0/CPU0:ROA#admin show license entitlement
```

```
Entitlement:
```

```
Tag: regid.2014-06.com.cisco.A9K-MOBILE-LIC,1.0_e447924c-0a6f-41be-9202-8ae60fcc2972,  
Version: 1.0, Not In Use  
Requested Time : NA, Requested Count: NA  
Vendor String:
```

```
Tag: regid.2014-09.com.cisco.A9K-IPSEC-20G-LIC,1.0_a165db99-eb3f-474b-bdf0-  
ce4b140d9b45, Version: 1.0, Not In Use
```

Requested Time : NA, Requested Count: NA
Vendor String:

Tag: INSTALLMGR, Version: 1.0, Not In Use
Requested Time : NA, Requested Count: NA
Vendor String:

Tag: regid.2014-04.com.cisco.A9K-24X10-OPT-LIC,1.0_66d3ccf7-a374-4409-a3f9-6bc56d645f1c, Version: 1.0, Enforce Mode: Out of compliance
Requested Time : Mon Jan 12 2015 20:47:07 PST, Requested Count: 1
Vendor String:
... output snipped ...

Vérifiez la conformité aux licences.

RP/0/RSP0/CPU0:ROA#**admin show license status**
Compliance Status: Out of compliance

Contrôle qui le groupe est en activité.

RP/0/RSP0/CPU0:ROA#**admin show licence pool**
Assigned Pool Info: PATRICK_NO_LIC

Chcek le certificat d'autorisation.

RP/0/RSP0/CPU0:ROA#**admin show license cert**
Licensing Certificates:

ID Cert Info:

Start Date: Mon Jan 12 2015 21:00:13 PST. Expiry Date: Tue Jan 12 2016 21:00:13 PST
Serial Number: 24724
Version: 3
Subject/SN: 60fe47f8-aaaa-40fc-ae3e-fae9c7b6d0ac
Common Name: 138091632beb1f2e38069e9eec8f9c626de471ac::1,2

Signing Cert Info:

Start Date: Wed Sep 11 2013 12:05:34 PST. Expiry Date: Sun May 30 2038 12:48:46 PST
Serial Number: 3
Version: 3

Vérifiez la version d'autorisation.

RP/0/RSP0/CPU0:ROA#**admin show license version**
Cisco Smart Licensing Agent, Version 1.1.4_throttle/16

Cette commande montre que les statistiques sur la Fonction Call Home tentent, qui a réussi et/ou a manqué.

RP/0/RSP1/CPU0:ROA#**show call-home smart-licensing statistics**

Success: Successfully sent and response received.
Failed : Failed to send or response indicated error occurred.
Inqueue: In queue waiting to be sent.
Dropped: Dropped due to incorrect call-home configuration.

Msg Subtype Success Failed Inqueue Dropped Last-sent (GMT-08:00)

Msg Subtype	Success	Failed	Inqueue	Dropped	Last-sent (GMT-08:00)
ENTITLEMENT	1	0	0	0	2014-12-17 21:08:35
DEREGISTRATION	1	0	0	0	2014-12-17 14:33:17
REGISTRATION	1	0	0	0	2014-12-17 21:07:53
ACKNOWLEDGEMENT	1	0	1	0	2014-12-17 21:08:09
RENEW	1	0	0	0	2014-12-17 21:08:57

Processus de Fonction Call Home

Vérifiez les fichiers de suivi pour le processus de *call_home* ensuite, puisque le transport entre l'ASR9K et le nuage de Cisco est géré par lui.

```
RP/0/RSP0/CPU0:ROA#show call-home trace error last 2
```

```
81 wrapping entries (576 possible, 320 allocated, 0 filtered, 81 total)!  
Jan 28 10:10:29.729 call_home/error 0/RSP0/CPU0 t10 call_home_http_resp_data(),  
httpc response error, Host name resolution failed
```

```
Jan 28 10:10:39.730 call_home/error 0/RSP0/CPU0 t19 call_home_events_handler() failure status 67
```

Contrôle de Smartlic (agent logiciel)

Vérifiez les suivis smartlic. Ces suivis indiquent l'interaction de permis avec des serveurs de nuage de Cisco.

```
RP/0/RSP0/CPU0:ROA#admin show license trace smartlic last 2
```

```
987 wrapping entries (1088 possible, 0 filtered, 987 total)  
Jan 28 20:10:36.245 smartlicense/smartlic 0/RSP0/CPU0 t3 [2302054]  
Failed to bind to SysDB - 'Subsystem(2091)' detected the 'success' condition  
'Code(45)': Unknown Error(292)
```

```
Jan 28 20:10:36.245 smartlicense/smartlic 0/RSP0/CPU0 t3 [2302054]  
SMART ERROR - SASACKExpirationJob: expirySeconds=3842
```

Contrôle de processus de Licmgr

Ce processus est l'interface principale à l'autorisation intelligente sur l'ASR9K et a considéré la colle entre de divers composants.

```
RP/0/RSP1/CPU0:ROA#admin show license trace
```

```
557 wrapping entries (576 possible, 0 filtered, 5403 total)  
Dec 17 13:08:18.358 license/licmgr 0/RSP1/CPU0 t3 [3125351] SLA Debug :  
Client search success pkg/bin/rsi_agent (No error)  
Dec 17 13:08:18.358 license/licmgr 0/RSP1/CPU0 t3 [3125351] SLA Debug :  
A9K-MOD160-AIP-SE regid.2014-06.com.cisco.A9K-MOD160-AIP-SE,  
1.0_7f1b3d9c-a183-41d1-8d0b-d98dcc2751a8 (No error)
```

Suivis de personne à charge de plate-forme

Bien que la pièce dépendante de plate-forme (palladium) du code soit juste une bibliothèque de liens dynamiques, elle a un important rôle en déclenchant des demandes de l'autorisation de permis. Par conséquent il résout des problèmes quant aux types de licence, des comptes, et ainsi de suite.

```
RP/0/RSP1/CPU0:ROA#admin show license trace platform all last 5
```

```
1849 wrapping entries (5440 possible, 3136 allocated, 0 filtered, 183450 total)  
Dec 17 20:43:33.480 vkg_lic/audit 0/RSP1/CPU0 t1 Agent Client Audit Cmd Start: ver:1,  
node:0x00000041 cmd:Audit(5) req:Mobile(9) feature:A9K-MOBILE-LIC(13) grant:  
Not Pending(0)  
Dec 17 20:43:33.480 vkg_lic/audit 0/RSP1/CPU0 t1 Agent Client Audit Cmd Start #2:  
client restarted:False up for a day:True  
Dec 17 20:43:33.480 vkg_lic/audit 0/RSP1/CPU0 t1 AUDIT Reply License Start:
```

```
request:Mobile(9) slot:4 grant:Not Pending(0)
Dec 17 20:43:33.480 vkg_lic/audit 0/RSP1/CPU0 t1 AUDIT Reply License End:
request:Mobile(9) slot:4 grant:Not Pending(0) rc: 0x00000000 No error
Dec 17 20:43:33.480 vkg_lic/audit 0/RSP1/CPU0 t1 Agent Client Cmd End:Audit(5),
slot:4 rc:0x00000000 No error
```

Activez le debug

Si tout le reste échoue, alors activez le débogage et écrivez une demande sur demande du renouvellement des Certificats ou des autorisations. Ceci mettront au point devrait collecter toutes les transactions entre l'ASR9K et les services en nuage de Cisco.

```
RP/0/RSP0/CPU0:ROA#debug smartlic
RP/0/RSP1/CPU0:ROA#show debug
```

```
#### debug flags set from tty 'aux0_RSP1_CPU0' ####
smartlic debug flag is ON with value 0
```

Aucune élimination des imperfections directe de serveur de nuage UI/Cisco n'est disponible. Envoyez un email à asr9k-smart-lic@cisco.com avec toutes les questions.

Chance et extrémités

1. Quand de plusieurs cases sont configurées pour saisir l'autorisation du même GROUPE de PERMIS, même si seulement UN périphérique est court par UN permis, alors TOUS vos périphériques sont OOC. C'est principalement dû à la conception qui a le point de vue du groupe comme conteneur. Le nouveau modèle, l'organisation hiérarchique des groupes qui est dans les travaux, adresse le comportement dans des versions futures.
2. Envoyez-vous n'importe quelle **sortie de commande show** directement de la console. Notez les guillemets et l'utilisation du point-virgule après chaque commande. La Fonction Call Home fait beaucoup d'exécutions qui ne sont pas autorisation intelligente associée. C'est un exemple pour de quelle Fonction Call Home pourrait être utilisé. C'est une configuration en cours qui peut être modifiée pour n'importe quel environnement.

```
RP/0/RSP1/CPU0:ROA#show run call-home
call-home
service active
site-id BUILDING20-125
sender reply-to pasoltan@cisco.com
sender from roa@cisco.com
alert-group syslog
alert-group snapshot
alert-group inventory
mail-server 171.68.58.10 priority 10
mail-server 173.37.183.72 priority 20
mail-server 2001:420:303:2008::24 priority 2
mail-server mybastion.cisco.com priority 1
phone-number +1-408-526-8438
contact-email-addr sch-smart-licensing@cisco.com
street-address 1550 E.Tasman Drive, San Jose, CA 9513
profile CiscoTAC-1
active
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
reporting smart-call-home-data
reporting smart-licensing-data
destination transport-method http
```

```
RP/0/RP1/CPU0:ROA#call-home send "show run call; admin show platform"
```

email pasoltan@cisco.com msg-format long-text

Sending ondemand CLI output call-home message ...
Please wait. This may take some time ...

3. La commande **smartlic d'état de show call-home** succès utilise mot les « qui signifie simplement d'un point de vue de processus de Fonction Call Home que le transport des messages de l'ASR9K aux serveurs de nuage de Cisco était réussi. Cependant, ceci ne signifie pas que l'exécution d'autorisation de bout en bout avec des serveurs de nuage de Cisco était réussie. Par exemple, s'il y a une question avec le compte, certificat, ou ainsi de suite avec le portail, la Fonction Call Home transporte le message et affiche le succès, mais toute l'exécution de contrôler les permis par les serveurs principaux pourrait échouer.

```
RP/0/RSP1/CPU0:ROA#show call-home smart-licensing statistics
Success: Successfully sent and response received.
Failed : Failed to send or response indicated error occurred.
Inqueue: In queue waiting to be sent.
Dropped: Dropped due to incorrect call-home configuration.
```

Msg Subtype	Success	Failed	Inqueue	Dropped	Last-sent (GMT-08:00)
ENTITLEMENT	1	0	0	0	2014-12-17 21:08:35
DEREGISTRATION	1	0	0	0	2014-12-17 14:33:17
REGISTRATION	1	0	0	0	2014-12-17 21:07:53
ACKNOWLEDGEMENT	1	0	1	0	2014-12-17 21:08:09
RENEW	1	0	0	0	2014-12-17 21:08:57

4. Quand vous configurez les interfaces de gestion avec l'ipv4 et l'IPv6, la commande de la résolution des noms à la résolution d'adresse IP ou de DN est IPv6 d'abord.

```
RP/0/RSP1/CPU0:ROA#show run int M*
interface MgmtEth0/RSP0/CPU0/0
cdp
ipv4 address 172.27.130.64 255.255.255.128
ipv6 address fe80::172:27:130:64 link-local
ipv6 address 2001:420:303:2008:0:28:1:64/80
... snipped output ...
```

```
RP/0/RSP1/CPU0:ROA#ping tools.cisco.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:420:1201:5::a, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/45/49 ms
```

```
RP/0/RSP1/CPU0:ROA#ping tools.cisco.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:420:1201:5::a, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/45/49 ms
```

[Informations connexes](#)

- [Guide utilisateur de Smart Call Home](#) - HTML
- [Guide utilisateur de Smart Call Home](#) - PDF
- [Sécurité de Smart Call Home](#)
- [Communauté de soutien Cisco](#)
- [Vidéo : Configurez la Fonction Call Home](#)
- [Commandes intelligentes d'autorisation](#) - HTML
- [Commandes intelligentes d'autorisation](#) - PDF
- [Les informations générales : Autorisation intelligente](#)

- [Foire aux questions intelligente d'autorisation](#)
- [Guide de passerelle de transport](#)
- [Foire aux questions de passerelle de transport](#)
- [Support et documentation techniques - Cisco Systems](#)